(12) UK Patent Application (19) GB (11) 2 261 538 (13) A

(43) Date of A publication 19.05.1993

(21) Application No 9124124.0

(22) Date of filing 13.11.1991

(51) INT CL[5]
G07F 19/00 7/10

(52) UK CL (Edition L)
G4H HTG H1A H13D H14A H14B

(56) Documents cited
GB 1458646 A WO 86/03040 A1 US 5023908 A

(58) Field of search
UK CL (Edition K) G4H HTG
INT CL[5] G07F

(71) Applicant
The Governor and Company of The Bank of Scotland

(Incorporated in the United Kingdom)

Head Office, The Mound, Edinburgh, Scotland, EH1 1YZ, United Kingdom

(72) Inventor
James Carden

(74) Agent and/or Address for Service
Cruikshank & Fairweather
19 Royal Exchange Square, Glasgow, G1 3AE, United Kingdom

(54) Transaction authentication system

(57) A transaction authentication system comprises a microchip card and a terminal. The card has a memory for storing PIN data and transaction sequence data. A processor increments the transaction sequence data each time the card is used in a transaction, and combines and encrypts the incremented transaction sequence data and a given PIN data component to provide a unique transaction signature. The given PIN data component and the encryption key used in the generation of the transaction signature comprise a secret component personal to the user but concealed from the user and known only to the authoriser. The transaction signature and the incremented transaction sequence data are displayed/printed/transmitted. A transaction may be authenticated by means of the authoriser decoding the transaction signature using the incremented transaction sequence data and an appropriate decryption key so as to extract PIN data component material, then comparing it with that belonging to the card holder.

GB 2 261 538 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

The claims were filed later than the filing date within the period prescribed by Rule 25(1) of the Patents Rules 1990.

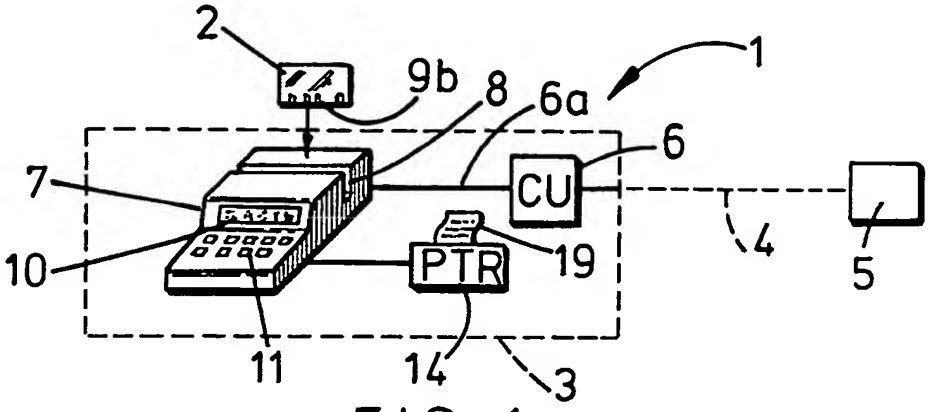

FIG. 1

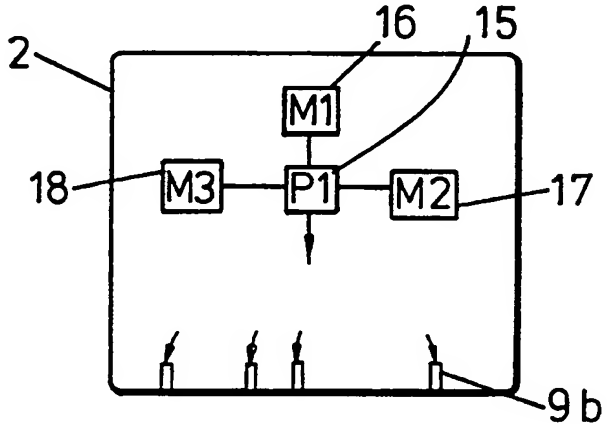

FIG. 2

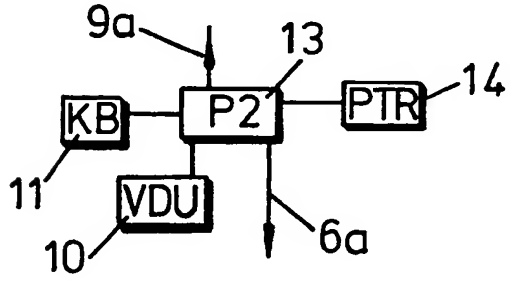

FIG. 3

TRANSACTION AUTHENTICATION SYSTEM

The present invention relates to security systems for transaction cards, and in particular to a system for authenticating individual transactions.

Transaction cards are very widely used as an alternative to cash and invariably contain various features to counteract fraudulent use thereof. The card issuers and transaction authorisors however continue to suffer substantial losses due to by counterfeiting of security features whether they be cardholder signatures, holographic devices or magnetic stripes on transaction documentation or invalid cards as appropriate. The PIN (Personal Identification Number) number is acknowledged as a useful way of reducing such losses but its usage is generally limited to Automated Teller Machines (ATMs) designed to hold securely, sensitive data such as encryption keys. PINs are not widely used at Point of Sale terminals because of the complexity of managing them adequately in such a potentially insecure environment. Various increasingly sophisticated and complex, not to mention expensive, features continue to be added to transaction cards to minimise the possibility of tampering therewith but there remains a major technical problem in finding an effective way to authenticate individual transactions, that is, to identify and distinguish valid transactions from

unauthorised ones.

The present invention provides a transaction authentication system comprising a microchip card, a terminal means having card interface means for transferring data between said card and said terminal means, said microchip card having memory means for storing PIN data, at least one of said card and said terminal means having a user input interface for user entry of a PIN data component known to the user, at least one of said card and terminal means having processor means formed and arranged for comparing the stored user-known input PIN data component with the user entered PIN data component and producing an output validation signal in response to entry of a valid user PIN data component, at least one of said card and said terminal means including validation signal output means directly or indirectly drivable by said validation output signal so as to provide user-sensible confirmation of valid PIN data component entry, characterised by said microchip card having memory means for storing transaction sequence data and said processor means being further formed and arranged for incrementing the transaction sequence data in a predictable manner each time the card is used in a transaction, and for combining the incremented transaction sequence data and a given PIN data component, at least one of said card

and said terminal means including memory means holding an encryption key for encryption of the combined transaction sequence data and given PIN data component in a predictable manner so as to provide a unique transaction signature, at least one of said given PIN data component and the encryption key used in the generation of the transaction signature comprising a secret component personal to the user but concealed from the user and known only to the authorisor, at least one of said card and terminal means having transaction signal output means formed and arranged for providing an output signal containing the encoded transaction signature and the incremented transaction sequence data, whereby in use of the system a transaction may be authenticated by means of the authorisor decoding the encoded transaction signature using the incremented transaction sequence data and an appropriate decryption key so as to extract PIN data component material contained therein, and comparing the extracted PIN data component material with that belonging to the card holder.

Thus with a transaction authentication system of the present invention the microchip card is effectively modified in a predictable but secure manner each time it is used so that for each transaction it will function as a "new" card and generate not only an incremented

transaction sequence data but also a substantially unique encoded transaction signature which can subsequently be decoded by the authorisor with the aid of an appropriate decryption key. The corresponding incremented transaction sequence data, and appropriate PIN data component material, are distinguished from transaction signatures generated by "unauthorised" cards, that is, forged cards having an incorrect personal secret PIN data component or encryption key, or stolen or misused cards in which the incremented transaction sequence data does not relate in an acceptable manner to the transaction sequence data of any properly used card held by the user. Thus the present invention provides a particularly high degree of security to the Authorisor, without requiring any change in operation by the user, and necessitating only, in the case of off-line transactions, recordal of the incremented transaction sequence data and encoded transaction signature which can in any event be automated if desired. Moreover, by means of incorporating magnetic stripe emulation in the card (e.g. in a form such as that previously known from and described in EP-A-0 203 683) it is possible to use substantially conventional magnetic reader transaction terminals. It will be appreciated though that other suitable forms of card interface means may also be employed in accordance with the present invention

including suitable direct electrical contact means as will be further explained hereinbelow.

In one embodiment of the present invention the given PIN data component used in generating the transaction signature is simply the PIN data component known to the user and used by him/her in the normal way. In this case the secret personal encryption key will of course have to be stored on the card. In another, preferred, embodiment though there is used a secret personal PIN data component, stored on the card in addition to the user-known PIN data component, in the generation of the transaction signature. In this latter case, there may be used a "public" encryption key common to all users and possibly also common to different authorisors, and this may be stored either on the card or in the transaction card terminal means. If desired though a secret personal PIN data component system could be used in combination with a secret personal encryption key system to provide even greater security (both the secret personal PIN data component and encryption key being stored on the card).

Any suitable type of encryption key may be used including, for example, an RSA encryption key. Moreover there may be used an encryption of the type which can be used for both encoding and decoding or a more complex

type which required the use of a separate decryption key for decoding of the transaction signature.

Further preferred features and advantages of the invention will appear from the following detailed description given by way of example of a preferred embodiment illustrated with reference to the accompanying drawings, in which:-

Fig. 1 is a generally schematic representation of a transaction authentication system of the invention in use in on-line mode;

Fig. 2 is a more detailed view of the transaction card of the system of Fig. 1; and

Fig. 3 is a detailed block diagram of the input/output device of the terminal means of the system of Fig. 1.

Fig. 1 shows a transaction authentication system 1 comprising a microchip card 2 and a terminal means 3 connected (e.g. via a telephone line) 4 to a remote main-frame computer 5. In more detail the terminal means 3 comprises a generally conventional transaction card reader and communications unit 6 for reading data stored in the magnetic stripes of conventional transaction cards and communicating with a remote main-frame 5, said unit 6 having an external signal input connection 6a to a transaction card input/output device 7 for reading from and writing to the transaction

card 2 of the present invention.

The I/O device 7 has a card receiving slot 8 provided with complementary electrical contact means 9a (see Fig. 3) for coupling with direct electrical contact means 9b on the card 2. Desirably the electrical contact means 9a, 9b are formed and arranged in accordance with a suitable ISO standard for microchip card readers. In addition the I/O device 7 has a visual display means conveniently in the form of an LCD device 10 and a keyboard 11 for allowing user entry of PIN data etc. As shown in Fig. 3, the keyboard 11 and display device 10 are connected to an I/O device processor 13 which is also connected to a "hard copy" printer device 14, and to the communications unit 6.

The card 2 as shown in Fig. 2 has a processor 15 connected to the card contact means 9b and also to memory storage means comprising a first memory (conveniently E^2PROM type) 16 for storing both user-known and secret personal PIN data components, second memory means conveniently (in the form of ROM type memory) 17 for storing encryption and other programs used in the operation of the card (see below), and third memory means (conveniently of RAM type) 18 for holding transaction sequence data.

The processor means 13,15 and programs used are formed and arranged so that in use when a card 2 is inserted in the card receiving slot 8 of the I/O device 7 and the card user enters his/her (user-known) PIN data component via the keyboard 11, the I/O device processor 13 transmits this to the card processor 15 which compares it with the value stored in the first card memory 16 and then sends back to the I/O device processor 15, a suitable signal which generates a "VALID" or "INVALID" output signal on the I/O device display 10.

The merchandisor or other operator of the terminal means 13 can then enter details of the transaction in the terminal means 3 in generally known manner and activates the I/O device processor 13 to send a signal to the card processor 15 to increment the transaction sequence data in the third memory means 18. The incrementation could be simply linear but more desirably would be controlled by a more or less complex algorithm in order to frustrate to a greater or lesser extent fraudulent generation of transaction sequence data.

The card processor 15 then combines the newly incremented transaction sequence data with the secret PIN data component (which may also conveniently be referred to as a secondary card reference value or SCRV) held in the first memory means 16 and encodes it by

means of the encryption key (which may be of any suitable kind e.g. an RSA type key) held in the second memory means 17 so as to generate a transaction signature in a suitable format such as a 512 bit string of cyphertext. Again the combination of the transaction sequence data with the SCRV may be in a simple arithmetical manner or, more desirably, in accordance with a more or less complex algorithm in order to increase the overall security of the process.

The card processor 15 then sends the incremented transaction sequence data and the encoded transaction signature to the I/O device processor 13 which then displays these on the I/O device display 10 for transcription by the terminal means operator and subsequent return to the card authorisor as and when required to authenticate the transaction concerned. In view of the length and complexity of the transaction signature, in practice only part, e.g the first 8 characters. i.e. the hexadecimal representation of the first 32 bits of the cyphertext would normally be used in this type of operational mode. Alternatively or additionally the incremented transaction sequence number and the encoded transaction signature are output to the printer 14 for recording with other conventional transaction data on the till receipt 19 or other transaction documentation, with conveniently one copy

going to the card holder and one being retained by the operator for return to the card authorisor again as and when required for authentication purposes. In this case normally the full 64 character form of the transaction signature would be recorded in the above example of transaction signature format. Advantageously though the terminal means is operated on on-line mode so that the incremented transaction sequence data and encoded transaction signature are transmitted immediately to the card authorisor's main computer 5 for comparison of the transaction sequence data with earlier authentic transaction sequence data to judge whether the newly incremented transaction sequence data is within the range of reasonably expected values for an authentic incremented transaction sequence data for that particular card (allowing of course for the fact that certain off-line transactions may not yet have been logged on the main computer 5). Also the encoded transaction signature 13 decoded using the associated transaction sequence data and an appropriate decryption key in order to extract an SCRV which can then be compared with the value held on the main computer 5 for the card holder whose identity will also have been entered at the terminal means 3 by the operator and transmitted to the authorisor's main computer 5 in conventional manner. The main computer 5 will then send back to the terminal means 3 a suitable signal for

display of a message on the display means 7 acknowledging or rejecting the authenticity of the transaction.

Various modifications may be made to the above system without departing from the scope of the present invention. Thus other conventional security features such as holograms may be employed on the surface of the card. Also the microchip should desirably be embedded in the card in such a way as to substantially prevent the possibility of replacement of the card without serious damage to the card. Furthermore there could be used an encryption key which would allow subsequent decryption of the encoded transaction signature at different levels, e.g. decryption of the full signature with a simplified public or general decryption key and decryption of part (only) of the signature using a full secret decryption key which may moreover be personal to the individual card holder.

CLAIMS

1. A transaction authentication system comprising a microchip card, a terminal means having card interface means for transferring data between said card and said terminal means, said microchip card having memory means for storing PIN data, at least one of said card and said terminal means having a user input interface for user entry of a PIN data component known to the user, at least one of said card and terminal means having processor means formed and arranged for comparing the stored user-known input PIN data component with the user entered PIN data component and producing an output validation signal in response to entry of a valid user PIN data component, at least one of said card and said terminal means including validation signal output means directly or indirectly drivable by said validation output signal so as to provide user-sensible confirmation of valid PIN data component entry, characterised by said microchip card having memory means for storing transaction sequence data and said processor means being further formed and arranged for incrementing the transaction sequence data in a predictable manner each time the card is used in a transaction, and for combining the incremented transaction sequence data and a given PIN data component, at least one of said card and said terminal means including memory means holding

an encryption key for encryption of the combined transaction sequence data and given PIN data component in a predictable manner so as to provide a unique transaction signature, at least one of said given PIN data component and the encryption key used in the generation of the transaction signature comprising a secret component personal to the user but concealed from the user and known only to the authorisor, at least one of said card and terminal means having transaction signal output means formed and arranged for providing an output signal containing the encoded transaction signature and the incremented transaction sequence data, whereby in use of the system a transaction may be authenticated by means of the authorisor decoding the encoded transaction signature using the incremented transaction sequence data and an appropriate decryption key so as to extract PIN data component material contained therein, and comparing the extracted PIN data component material with that belonging to the card holder.

2. A system according to claim 1 wherein said terminal card interface means is in the form of direct electrical contact means.

3. A system according to claim 1 or claim 2 wherein said PIN data component is the PIN data component known to the user.

4. A system according to claim 1 or claim 2 wherein said PIN data component is a secret personal PIN data component, stored on the card in addition to the user-known PIN data component.

5. As system according to any one of claims 1 to 4 wherein said encryption key is common to all users and is stored on the card.

6. A system according to any one of claims 1 to 4 wherein said encryption key is stored in the terminal means.

7. A system according to any one of claims 1 to 6 wherein said encryption key is an RSA type encryption key.

8. A system according to any one of claims 1 to 6 wherein said encryption key is of the encoding and decoding type.

9. A system according to any one of claims 1 to 6 wherein said encryption key is of the type requiring a separate decryption key for decoding of the transaction signature.

10. A system as claimed in claim 1 wherein said card has incorporated therein magnetic stripe emulation usable in a substantially conventional magnetic reader transaction terminal.

11. A transaction authentication system substantially as described hereinbefore with particular reference to Figs. 1 to 3 of the accompanying drawings.

Patents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
GB 9124124.0

Relevant Technical fields

(i) UK Cl (Edition K) G4H (HTG)

(ii) Int Cl (Edition 5) G07F

Search Examiner
M J DAVIS

Databases (see over)

(i) UK Patent Office

(ii)

Date of Search
2 DECEMBER 1992

Documents considered relevant following a search in respect of claims 1-11

Category (see over)	Identity of document and relevant passages		Relevant to claim(s)
X	GB 1458646 A	(OMRON) especially page 2 lines 5-45, page 7 lines 7-14	1-3, 5-10
X	WO 86/03040 A1	(INTELLICARD) especially pages 13-16, page 24 line 15 to page 25 line 37, page 28 line 32 to page 30 line 9	1-3, 5-10
X	US 5023908 A	(WEISS) especially column 2 lines 21-42, column 3 line 7 to column 4 line 28	1-11

Category	Identity of document and relevant passages	Relevant to claim(s)

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).

Published 1993 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from Sales Branch, Unit 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.